

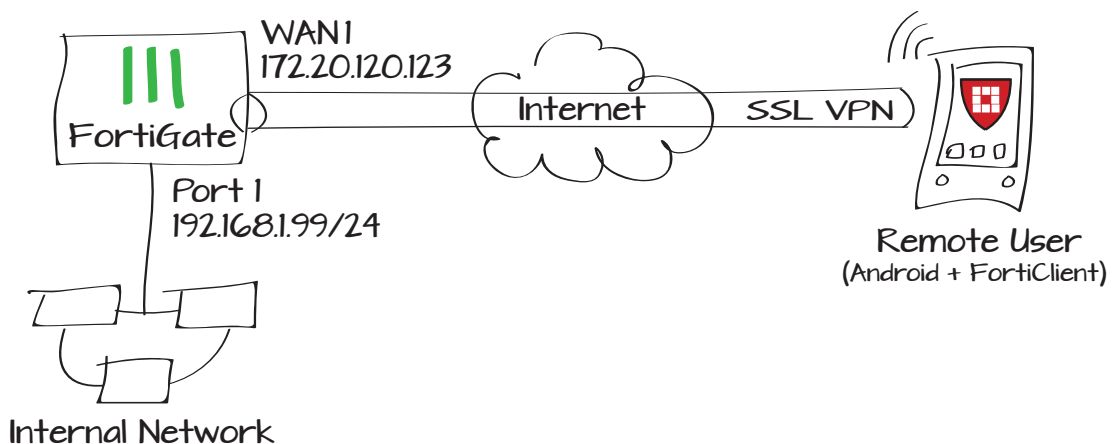
# Connecting an Android to a FortiGate with SSL VPN

This recipe describes how to provide a group of remote Android users with secure, encrypted access to the network using FortiClient and SSL VPN.



You must download the FortiClient application from the Play Store and install it on your Android device. Refer to the [FortiClient for Android QuickStart Guide](#). This recipe was tested using Android version 4.3.

1. Creating an SSL VPN tunnel for remote users
2. Creating a user and a user group
3. Adding an address for the network
4. Adding security policies for access to the Internet and internal network
5. Configuring the tunnel on FortiClient for Android
6. Results



# Creating an SSL VPN tunnel for remote users

Go to **VPN > SSL > Portal**.

Edit the full-access portal.

The full-access portal allows the use of tunnel mode and/or web mode. In this scenario we are using both modes.

**Enable Split Tunneling** is *not* enabled so that all Internet traffic will go through the FortiGate unit and be subject to the corporate security profiles.

Select **Create New** in the **Include Bookmarks** area to add a bookmark for a remote desktop link/connection.

Bookmarks are used as links to internal network resources.

Name:full-access

Portal Message:Welcome to SSL VPN Service

Theme:Blue

Page Layout:

☒ Enable Tunnel Mode

☐ Enable Split Tunneling

IP Pools

SSLVPN\_TUNNEL\_ADDR1

Client Options

☐ Save Password☐ Auto Connect☐ Always Up (Keep Alive)

☒ Enable Web Mode

Applications

☒ HTTP/HTTPS☒ SSH☒ CITRIX

☒ FTP☒ TELNET☒ RDP NATIVE

☒ RDP☒ VNC☒ Port Forward

☒ SMB/CIFS☒ PING

☒ Include Session Info☒ Include Connection Tool☒ Include FortiClient Download☒ Include Bookmarks

Create NewEdit SSL-VPN PortalDelete

Name	Type	Location	Description
No matching entries found			

☒ Prompt Mobile Users to Download FortiClient App☒ Allow Multiple Concurrent Sessions For Each User

View Portal

CategoryRemote desktop

NameWindows server

TypeRDP

Location192.168.1.114

Screen Width1024

Screen Height768

Logon User

Logon Password

Keyboard LayoutEnglish, US

Description

Full Screen Mode☒

# Creating a user and a user group

Go to **User & Device > User > User Definition.**

Add a remote user with the User Creation Wizard (in the example, 'twhite').

1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info 4 Provide Extra Info

☒ Local User  
☐ Remote RADIUS User  
☐ Remote TACACS+ User  
☐ Remote LDAP User

< Back Next > Cancel

1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info 4 Provide Extra Info

User Name twhite  
Password .....

< Back Next > Cancel

1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info 4 Provide Extra Info

Email Address twhite@example.com  
☒ SMS  
Phone Number 555555555  
Service Type FortiGuard Messaging Service

< Back Next > Cancel

1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info 4 Provide Extra Info

☒ Enable  
☐ Two-factor Authentication  
☐ User Group

< Back Done Cancel

Go to **User & Device > User > User Groups.**

Add the user to a user group for SSL VPN connections.

Name sslvpn\_group

Type ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Available Users

Members

- Local Users - guest

- Local Users - twhite

# Adding an address for the network

Go to **Firewall Objects > Address > Addresses.**

Add the address for the local network. Set **Type** to **Subnet**, **Subnet/ IP Range** to the local subnet, and **Interface** to an internal port.

# Adding security policies for access to the Internet and internal network

Go to **Policy > Policy > Policy.**

Add a security policy allowing access to the internal network. Set **Type** to **VPN** and **Subtype** to **SSL-VPN.**



If your FortiGate unit does not have the Policy-based IPsec feature turned on, you will only have to set **Policy Type** to **VPN.**

Set **Incoming Interface** to your Internet-facing interface, **Local Interface** to an internal port and **Local Protected Subnet** to the address for the local network. Create a new **Authentication Rule** to allow the remote user group access.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Local LAN

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.1.0/255.255.255.0

Interface

port1

Show in Address List

☒

Comments

Write a comment...

0/255

Policy Type

☐ Firewall ☒ VPN

Policy Subtype

☐ IPsec ☒ SSL-VPN

Incoming Interface

wan1

Remote Address

all

Local Interface

port1

Local Protected Subnet

Local LAN

☐ SSL Client Certificate Restrictive

Cipher Strength

Any

Configure SSL-VPN Authentication Rules

Create New	Edit	Delete				
User/Group	Service	Schedule	UTM Security	SSL-VPN Portal	Logging	Action
sslvpn_group	ALL	always	-	full-access		✓ ACCEPT
ANY	ALL	always	-			⊘ DENY

Tags

Applied tags

Add tag

Comments

Write a comment...

0/1023

Add a second security policy allowing access to the Internet.

For this policy, **Incoming Interface** is *sslvpn tunnel interface* and **Outgoing Interface** is your Internet-facing interface.

# Configuring the tunnel on FortiClient for Android

Open FortiClient on your Android device and press **Settings**.

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

☒ Enable NAT

☒ Use Destination Interface Address

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

☐ Fixed Port

Click to add...

☒ Firewall ☐ VPN

☒ Address ☐ User Identity ☐ Device Identity

sslvpn tunnel interface

SSLVPN\_TUNNEL\_ADDR1

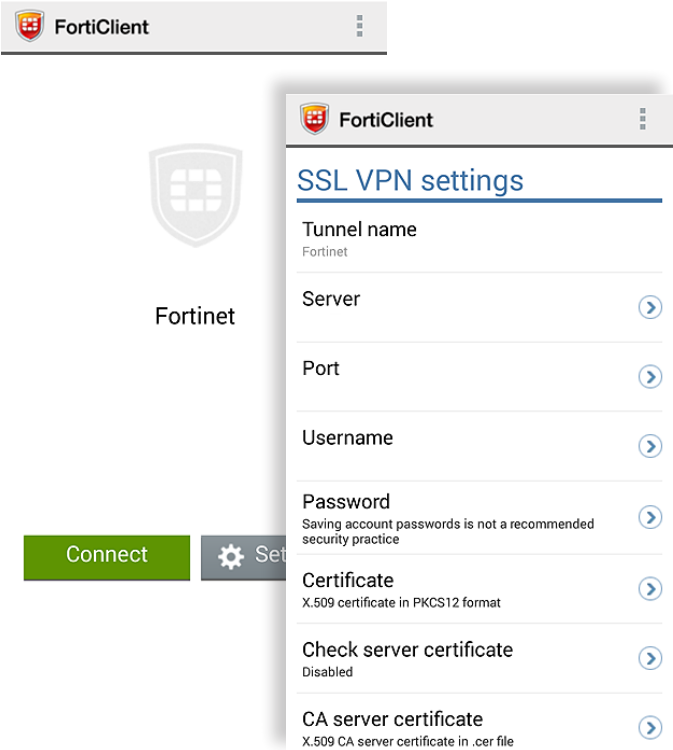
wan1

all

always

ALL

ACCEPT



Select **Server** to configure the server address.



If you changed the default SSL VPN port in the FortiGate, you must also change the **Port** setting on the Android device. Otherwise, leave the port as default.

Next, enter the **Username** and **Password** that you configured on the FortiGate.

Return to the main screen and press the **Connect** button.

Confirm the server connection and press the **Login** button.

Server

172.20.120.123

OK Cancel

Username

twhite

OK Cancel

Password

\*\*\*\*\*

OK Cancel

Connect Settings

Login Fortinet

twhite

\*\*\*\*\*

Login Cancel

FortiClient attempts to establish an SSL VPN tunnel with the FortiGate.

Once the SSL VPN tunnel is active, FortiClient shows the remote and local endpoints, and the duration of the current session.

With the tunnel active, the Android user can start their phone’s mail client or web browser and see content on the protected network.

To close the tunnel, press the **Disconnect** button.

On the FortiGate, verify the connection by navigating to **VPN > Monitor > SSL-VPN** and verify the list of SSL users.

The tunnel description indicates that the user is using tunnel mode.

FortiClient

Connecting to Fortinet

Cancel

Settings

FortiClient

Fortinet

Current Session: 0:02  
Remote: 172.20.120.81  
Local: 10.212.134.200

Disconnect

Settings

User	Source IP	Begin Time	Description
twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
Subsession		Tunnel IP:10.212.134.200	





User	Source IP	Begin Time	Description
twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
Subsession		Tunnel IP:10.212.134.200	

Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.







Go to **Log & Report > Traffic Log > Forward Traffic**.


Internet access occurs simultaneously through the FortiGate unit.

Select an entry to view more information.

Dst	192.168.1.114	Virtual Domain	root
Received	326664	Source Country	Reserved
Sent / Received	54.36 KB / 319.01 KB	Duration	83
Sent	55665	Application Details	
Group	N/A	Service	RDP
Protocol	6	User	 twhite
Destination Country	Reserved	Dst Port	3389
roll	65389	Status	
Timestamp	Wed Apr 17 14:17:15 2013	Tran Display	noop
Sequence Number	3618	Policy ID	11
Src Interface	wan1	Src	 twhite (172.20.120.23)
VPN	sslvpn_web_mode	Sent Packets	329
Level	notice 	VPN Type	sslvpn
Src Port	53820	Log ID	13
Sub Type	forward	Threat	
Received Packets	407	Date/Time	14:17:15 (Wed Apr 17 14:17:15 2013)
Dst Interface	unknown-0		

 Refresh  Download Raw Log

#	▾ Date/Time	▾ Src Interface	▾ Dst Interface	▾ Src	▾ Dst
▶ 1	14:26:05	ssl.root	wan1	10.212.134.200	 74.125.133.95
2	14:26:04	ssl.root	wan1	10.212.134.200	 173.194.77.94
3	14:26:04	ssl.root	wan1	10.212.134.200	 173.194.43.79
4	14:26:03	ssl.root	wan1	10.212.134.200	 66.171.121.34 (fortinet.c
5	14:25:57	ssl.root	wan1	10.212.134.200	 74.121.50.17 (www.page
6	14:25:44	ssl.root	wan1	10.212.134.200	 208.91.113.212
7	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30
8	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30
9	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30

Dst	 66.171.121.34 (fortinet.com)	Virtual Domain	root
Received	938	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	535 B / 938 B
Duration	17	Sent	535
Src NAT Port	54165	Application Details	
Service	HTTP	Protocol	6
Destination Country	United States	Dst Port	80
roll	65389	Status	close
Timestamp	Wed Apr 17 14:26:03 2013	Tran Display	snat
Sequence Number	8096	Policy ID	8
Src Interface	ssl.root	Src	10.212.134.200
Sent Packets	6	Level	notice 
Src Port	54165	Log ID	13
Sub Type	forward	Threat	
Received Packets	5	Date/Time	14:26:03 (Wed Apr 17 14:26:03 2013)
Dst Interface	wan1		